

⑪公開特許公報(A) 昭61-260735

⑫Int.Cl.

H 04 L 9/02
H 04 J 3/00

識別記号

厅内整理番号
Z-7240-5K
C-8226-5K

⑬公開 昭和61年(1986)11月18日

審査請求 未請求 発明の数 2 (全6頁)

⑭発明の名称 時分割マルチプルアクセス暗号通信方式

⑮特願 昭60-102017

⑯出願 昭60(1985)5月14日

⑭発明者	川崎 昱	川崎市中原区上小田中1015番地	富士通株式会社内
⑭発明者	妹尾 雅之	川崎市中原区上小田中1015番地	富士通株式会社内
⑭発明者	太田 幸一	川崎市中原区上小田中1015番地	富士通株式会社内
⑮出願人	富士通株式会社	川崎市中原区上小田中1015番地	
⑯代理人	弁理士 松岡 宏四郎		

明細書

1. 発明の名称

時分割マルチプルアクセス暗号通信方式

2. 特許請求の範囲

① 送信局がデータ送信用のバーストに同期碼を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期碼に予め定められた変更を所定回数実行することにより、前記バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う同期码を受信局に通知することを特徴とする時分割マルチプルアクセス暗号通信方式。

② 送信局がデータ送信用のバーストに同期碼を付加して送出する時分割マルチプルアクセス通信システムにおいて、前記送信局が前記同期碼に行う予め定められた変更の種類と、前記バーストに付加する暗号鍵を識別する情報との組合わせにより、該バーストにより伝送するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定することを特徴とする時分割マルチプルアセ

ス暗号通信方式。

3. 発明の詳細な説明

【概要】

送信局がデータ送信用のバーストに同期碼を付加して送出する時分割マルチプルアクセス(TDMA)通信システムにおいて、送信局が同期碼の変化を用いて暗号鍵の種類、更新時期を受信局に通知することにより、使用暗号鍵に関する情報量を削減するものである。

【産業上の利用分野】

本発明は時分割マルチプルアクセス通信システムを経由して暗号通信を行う時分割マルチプルアクセス暗号通信方式に関する。

暗号通信においては、送信側で送信データを予め定められた規約(以後暗号鍵と称する)に基づき暗号化して送信し、受信側で送信側と同一の暗号鍵に基づき復号化する。暗号化および復号化の為に使用する暗号鍵を複数種類準備し、適宜変更して使用することが、暗号化データの暗黙強度を向上する為に有効である。かかる場合に、送信側

FIRST AVAILABLE COPY

で使用している暗号鍵を受信側に認識させる必要がある。

この種の暗号通信を時分割マルチアクセス通信システムを経由して実行する場合には、送信側から受信側へ現在使用中の暗号鍵の種類を通知する情報量は、極力削減されることが望ましい。

【従来の技術】

第5図は時分割マルチアクセス衛星通信システムにおける従来ある時分割マルチアクセス暗号通信方式の一例を示す図であり、第6図は第5図におけるデータバーストの一例を示す図である。

送信局において、地上回線から地上回線接続インクフェース1を介してバースト組立部2に送信データDSが到着すると、バースト組立部2は、送信データDSを暗号化部3に伝達する。

暗号化部3は、暗号鍵発生部4が準備する複数種類(例えば2種類)の暗号鍵の中の、現在使用する暗号鍵に基づき送信データを暗号化し、バースト組立部2に伝達する。

3
生部BTを用いて復調し、バースト分解部11に伝達する。

バースト分解部11は、伝達されるデータバーストを分解し、同期語UWは同期語検出部12に伝達してバースト同期を確立させ、暗号化された送信データDSおよび暗号鍵識別情報KEYは復号化部13に伝達する。

復号化部13は、暗号鍵発生部4が準備する複数種類の暗号鍵の中から、受信した暗号鍵識別情報KEYに基づき、復号化に使用すべき暗号鍵を識別し、バースト組立部2から伝達された暗号化された送信データDSを識別した暗号鍵により復号化してバースト組立部2に伝達する。

バースト組立部2は、復号化部13から伝達された復号化された送信データDSを、地上回線接続インクフェース1を介して地上回線に伝達する。

【発明が解決しようとする問題点】

以上の説明から明らかな如く、従来ある時分割マルチアクセス暗号通信方式においては、送信局は送信データDSを暗号化するに使用した暗

バースト組立部2は、暗号化部3から伝達される暗号化された送信データDSに、送信局識別情報ID、暗号鍵発生部5から伝達される使用中の暗号鍵に関する識別情報(以後暗号鍵識別情報KEYと称する)、或いは同期語発生部5が作成するバースト同期確立用の同期語UW、更に受信局でデータバーストを受信するに必要な送信波再生部CR、ビット再生部BT、並びに誤り検出部分その他の補助部AUXを付加して第2図に示す如きデータバーストを組立て、同期語検出部6およびタイムスロット割当制御部7により指定される時間領域に、受調部8および送受信装置9を経由して衛星回線に伝達する。なお第2図におけるGTは、接続バーストとの衝突を防止するガード時間である。

一方受信局においては、復調部10が衛星回線から送受信装置9を経由して到着する信号の中から、同期語検出部6およびタイムスロット割当制御部7により指定された時間領域に受信したデータバーストを送信波再生部CRおよびビット再

4

号鍵を、暗号鍵識別情報KEYのみにより識別してデータバーストに付加していた。従って暗号鍵識別情報KEYの情報量が増加し、データバーストの他の情報を圧迫する恐れがあった。

【問題点を解決するための手段】

本発明は下記の手段を講ずることにより、前記問題点を解決する。

即ち本第一の発明においては、送信局が同期語に予め定められた変更を所定回数実行することにより、バーストにより伝達するデータの暗号化および復号化に使用する暗号鍵に所定の更新を行う時期を受信局に通知する。

また本第二の発明においては、送信局が同期語に予め定められた変更の種類と、バーストに付加する暗号鍵を識別する情報との組合せにより、バーストにより伝達するデータの暗号化および復号化に使用する暗号鍵の種類を受信局に指定する。

【作用】

即ち本第一の発明によれば、暗号鍵の更新時期

は同期語の変更により伝達される為、データペーストに付加すべき暗号部を識別する情報が不要となる。

また本第二の発明によれば、データペーストに付加すべき暗号部を識別する情報量の一部が同期語により伝達される為、暗号部を識別する情報の情報量が削減される。

〔実施例〕

以下、本発明の一実施例を図面により説明する。第1図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第2図は第1図におけるデータペーストの一例を示す図であり、第3図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図であり、第4図は第3図におけるデータペーストの一例を示す図である。なお、全図を通じて同一符号は同一対象物を示す。

第1図においては、送信局が暗号化に使用する暗号盤、および受信局が復号化に使用する盤は、暗号盤発生部4が予め準備するm種類の暗号盤を、

予め定められた順序で交換して使用するものとし、送信局および受信局において当初使用する暗号盤は、予め一致されているものとする。また同期語発生部5は複数種類（例えばm種類）の同期語UWを準備している。

また第2図においては、暗号盤識別情報KEYがデータペーストから除去されている。

送信局においては、ペースト組立部2が、地上回線から地上回線接続インターフェース1を介して伝達される送信データDSを暗号化部3により暗号化し、同期語発生部5が準備する同期語UWの中の所定の一個を選び、暗号盤再生部CR、ピット再生部BT、送信局識別情報ID、並びに誤り検出符号その他の補助部UXと共に、第4図に示す如きデータペーストを組立て、変調部8および送受信装置9を介して衛星通信回線に送信する。

送信局が現在使用中の暗号盤を次の暗号盤に更新する場合には、同期語UWの種類を予め定められた回数（例えば1回）変更して送信する。

一方受信局においては、ペースト分解部11が、

7

復調部10から伝達されるデータペーストを分解し、同期語UWは同期語検出部12に伝達してペースト同期を確立させ、暗号化された送信データDSは復号化部13に伝達する。なお同期語検出部12は、検出した同期語UWの種類を暗号盤発生部4および復号化部13にも伝達する。

復号化部13は、当初予め定められた暗号盤を用いて、ペースト組立部2から伝達された暗号化され送信データDSを識別した暗号盤により復号化してペースト組立部2に返送する。

なお同期語検出部12が伝達された同期語UWが変更されたことを識別すると、その旨暗号盤発生部4および復号化部13に通知する。暗号盤発生部4は変更回数が予め定められた回数（例えば1回）に達すると、先述使用していた暗号盤を次の暗号盤に更新し、暗号化部3および復号化部13に伝達する。以後復号化部13は、新たに変更された暗号盤を用いて、ペースト分解部11から伝達される暗号化された送信データDSを復号化する。

8

使って送信局から衛星通信回線に送信されるデータペーストには、暗号盤識別情報KEYを付加する必要が無くなる。

次に第3図においても、同期語発生部5は複数種類（例えばm種類）の同期語UWを準備している。

送信局においては、ペースト組立部2が、地上回線から地上回線接続インターフェース1に到着する送信データDSを暗号化部3により暗号化し、同期語発生部5が準備する同期語UWの中の所定の一個を選び、暗号盤発生部4から伝達される暗号盤識別情報KEY、暗号盤再生部CR、ピット再生部BT、送信局識別情報ID、並びに誤り検出符号その他の補助部UXと共に、第4図に示す如きデータペーストを組立てて、

なお暗号盤の識別は、暗号盤識別情報KEYおよび同期語UWの組合せで識別させる為、暗号盤識別情報KEYの種類は、第5図および第6図の場合に比し1/2に減少する。使ってデータペーストに付加すべき暗号盤識別情報KEYの所要

情報量(ビット数)も第2回に示す如く減少する。一方受信局においては、バースト分解部11が、復調部10から伝達されるデータバーストを分解し、同期語UWは同期語検出部12に伝達してバースト同期を建立させ、暗号化された送信データDSおよび暗号識別情報KEYを復号化部13に伝達する。なお同期語検出部12は、検出した同期語UWを復号化部13にも伝達する。

復号化部13は、暗号識別情報KEYと、同期語検出部12から伝達される同期語UWとの組合せに基づき、暗号発生部5が準備する復数種類(k種類)の暗号鍵の中から、復号化に使用すべき暗号鍵を識別し、バースト組立部2から伝達された暗号化された送信データDSを識別した暗号鍵により復号化してバースト組立部2に返送する。

なお、第1図乃至第4図はあく迄本発明の一実施例に過ぎず、例えばデータバーストの構成は図示されるものに限定されることは無く、他に多くの変形が考慮されるが、何れの場合にも本発明の

効果は変わらない。また送信局および受信局の構成は図示されるものに限定されることは無く、他に多くの変形が考慮されるが、何れの場合にも本発明の効果は変わらない。更に本発明の対象となる時分割マルチプルアクセス通信システムは、電磁波通信システムに限定されることは言う迄も無い。

【発明の効果】

以上本発明に上れば、前記時分割マルチプルアクセス通信システムにおいて、本第一の発明によれば、データバーストに付加すべき暗号鍵を識別する情報が不要となり、また本第二の発明によれば、データバーストに付加すべき暗号鍵を識別する情報量が削減され、データバースト内の他の情報量を圧迫する恐れが解消される。

4. 図面の簡単な説明

第1図は本第一の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第2図は第1図におけるデータバーストの一例を示す図、第3図は本第二の発明の一実施例による時分割マルチプルアクセス暗号通信方式を示す図、第

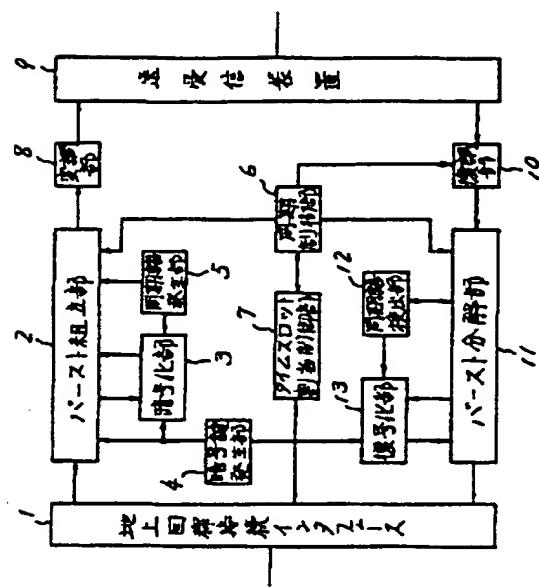
11

4図は第3図におけるデータバーストの一例を示す図、第5図は従来ある時分割マルチプルアクセス暗号通信方式の一例を示す図、第6図は第5図におけるデータバーストの一例を示す図である。

図において、1は地上回線接続インターフェース、2はバースト組立部、3は暗号化部、4は暗号鍵発生部、5は同期語発生部、6は同期制御部、7はタイムスロット割当制御部、8は変調部、9は送受信装置、10は復調部、11はバースト分解部、12は同期語検出部、13は復号化部、AUは補助部、BTはビット再生部、CRは差送波再生部、DSは送信データ、GTはガード時間、IDは送信局識別情報、KEYは暗号鍵識別情報、UWは同期語、を示す。

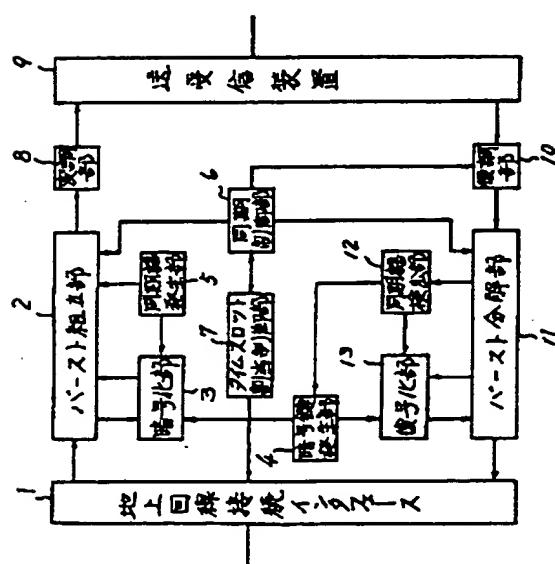
12

代理人 弁理士 佐藤宣四郎



本第2の照明の実施例を示す図
第3図

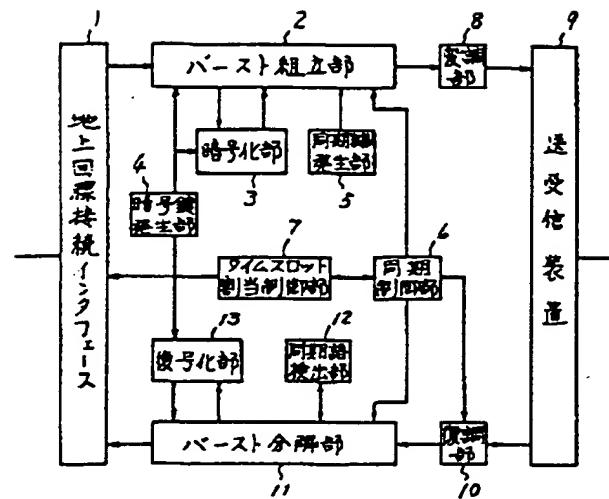
GT CR BT UW KEY ID DS AUX GT



本第1の照明の実施例を示す図
第1図

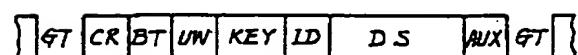
GT CR BT UW KEY ID DS AUX GT

本第2の照明の実施例を示す図
第4図



従来例を示す図

第5図



従来あるデータバーストと例示する図

第6図

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.